MOBILITY AIR FORCES
DISTRIBUTED MISSION OPERATIONS
PHYSICAL SECURITY GUIDE

23 March 2009

TIMOTHY S. SMITH, Col, USAF
Chief, Aircrew Operations and Training
Directorate of Air, Space & Information Operations
Headquarters, Air Mobility Command (AMC)

Physical Security Guideline for Mobility Air Forces (MAF)
Aircrew Training System (ATS) Facilities

The primary purpose of this guide is to assist in determining the breadth, scope, and cost of securing aircrew training facilities to participate in Distributed Mission Operations (DMO). Additionally, this guide should assist HQ AMC staff, local commanders, installation security program managers (ISPM), information assurance (IA) personnel, and civil engineering (CE) personnel in implementing appropriate physical security measures. This guide is based on direction contained in DoD 5200.1-R, DoD 8510.01, Mil-HDBK-1013/1A, TO-00-20F-2, UG-2045-SHR, AFI 31-101, AFI 31-401, AFI 33-201V1, AFI 33-203V1, AFI 33-203V3, AFI 33-200, AFI 33-210, AFI 71-101V3, and other applicable DoD directives. Local commanders are tasked under these regulations to ensure physical security standards adequately comply with these instructions. The security requirements for MAF DMO will drive the facility design and function requirements which may be more extensive than those of stand-alone facilities.

Assumptions

- DMO will take place at participating MAF Aircrew Training System (ATS) facilities. Security-in-depth already exists for operations on access-restricted military facilities.
- Given the nature of current and foreseen aircrew training, the Distributed Training Center (DTC) and participating ATS sites will be secured to operate at the collateral Secret level and below.
    - Site activity will include simulator operations, supporting maintenance functions, and operation of classified and unclassified stand-alone systems. Some of the stand-alone systems include Computer Based Training (CBT), Visual Threat Recognition and Avoidance Trainers (VTRAT), part-task trainers, and video teleconferencing capabilities.
    - Personnel who are part of the various ATS's have proper security clearances for access to classified and the need to know that information.
    - Sites that require operations above the Secret level are beyond the scope of this guide, and must address those physical security requirements using applicable directives.
- Participating ATS sites and the DTC will be assessed and modified, or built (in the case of new construction) to meet this guide.
- All simulators (IT Platforms), interconnections, stand-alone classified/unclassified systems and the DTC will be registered in the Enterprise Information Technology Data Repository (EITDR) and must meet the Certification and Accreditation (C&A) requirements listed in DoD 8510.01, the DoD Information Assurance Certification and Accreditation Process (DIACAP) and AFI 33-210, Air Force Certification and Accreditation Program (AFCAP).
- For the purposes of MAF aircrew training, two basic conditions exist for use of classified material: (1) continuous simulator operations in which systems software is inherently classified by its content or must be treated as classified due to the nature of the training (e.g., classified tactics), and (2) occasional (as

opposed to continuous) discussion or training with classified materials using amplified or non-amplified sound (e.g., VTRAT, classified CBT, and pre/post-training briefings).

Basic Guidance for Control and Storage of Classified Information

Agencies will establish control measures that limit access to classified information only to authorized personnel with a need to know. The access environment, along with the nature and volume of the information determine what measures are appropriate. Controls include technical, physical, and personnel measures. Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked GSA approved security container, vault, or a secure room/area constructed in accordance with DoD 5200.1-R, Appendix 7 and equipped with an IDS with personnel responding to the alarm annunciation. This guide deals primarily with technical and physical measures to meet the classified storage requirement through construction of a secure room or group of rooms (area) within a building; personnel measures may be used where physical/technical measures are impractical.

Definitions

Acoustical security - Sound attenuation measures employed for areas where discussion of classified information will take place. In ATS facilities this includes, as a minimum, Open Storage Areas, brief/debrief rooms, classrooms, classified VTC rooms and VTRAT rooms. When there is system amplification of classified information, sound attenuation measures must address amplified speech requirements. Discussion of classified material in unsecured areas without acoustical security measures in place is not permitted.

Emissions Security (EMSEC) - Standards for red/black separation of power and communications lines. Specific standards are not reproduced here due to classification. No classified electronic data in an unencrypted form shall be transmitted from the secure or attended area.

Open Storage Area - This is established when the volume or bulk of classified materials, or the functions associated with the processing of classified information, make the use of security containers impractical. It serves as the container for the storage of classified materials; security measures must be in place and maintained in order to ensure the integrity of the materials stored therein. By employing the following standards an area may be designated an Open Storage Area.

- Open Storage Areas for MAF ATS Sites will include:
    - Security-in-depth (inherent in facilities on established bases)
    - The physical perimeter meets the construction standards listed in Appendix 7 of DoD 5200.1-R (referenced below)

        - X-09 locks are required on the primary entrance door(s)
    - An intrusion detection system (IDS) which includes:
        - An integrated Card Access System (CAS)
        - Active balanced magnet strips (BMS) on the doors and windows, glass breakage detectors, and motion detectors within individual rooms that all report to base security forces
    - Acoustical Security shall be implemented for all Open Storage Areas. If, due to complexity or expense, an area inside an Open Storage Area cannot be secured acoustically, the area will have placards posted that identify it as an area where classified discussions are not permitted.
    - *The measures above are described in greater depth later in this document.*

- **Unattended Open Storage Area:** This condition exists whenever there are no personnel in the designated Open Storage Area. In this case all IDS systems and the X-09 locks must be engaged.

- **Attended Open Storage Area:** This condition exists when the Open Storage Areas is occupied. An open storage area must be occupied when the X09 locks are not engaged or motion detectors are disengaged for day to day operations. Other IDS components must still remain active.

Security-in-Depth: A determination that a security program consists of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement. Examples include the use of perimeter fences, employee/visitor access controls, use of intrusion detection systems, random guard patrols during non-working and working hours, and closed circuit video monitoring or other safeguards.

Simulator: For the purposes of this document, this is the Aircrew Training Device (ATD) which includes the host computer, visual system and Instructor Operator Station, plus any connected communication processor (s), environment generation system, or brief/debrief system. Any Loadmaster Station, Boom Operator Training Device, or Navigator Training Device which connects at any time to a Weapon System Trainer or Operational Flight Trainer which connects to the DTC is part of the overall simulator enclave.

Unsecured Area: An office setting or closed room not meeting Open Storage Area criteria. Standard building construction and alarming standards apply. Additionally, sound attenuation standards for classified discussion may still apply. All classified material not under the personal control of a properly cleared individual with a need to know must be properly stored in an approved GSA security container. Computer resources processing classified material in these areas will have removable hard drives that must be properly stored when not monitored. (e.g., SIPRNET drops, classified CBTs, VTRAT, etc.).

Physical Security Layout Options

Many variables impact the physical security layouts to be employed across the MAF ATS sites/facilities to assure adequate security. Two examples follow: (1) a Consolidated Option, and (2) a Compartmentalized Option. Either option, or a variation of these options, may be employed to meet individual, site-specific security requirements. Establishment of the Open Storage Area for a new or existing facility must minimize redundant, costly, and inefficient implementation of security measures. Regardless of the option chosen, the area that contains the participating simulator must be secured to Open Storage Standards.

From a security and operational perspective, the Consolidated Option is preferred, but not mandated. It may not be feasible or practical, or may be cost prohibitive. In such circumstances the Compartmentalized Option may have to be employed.

1. **Consolidated Option:** Situation in which all classified operations (as listed in the Assumptions) within an ATS are consolidated within the Open Storage Area. This option provides the most flexibility for operations since all processes may run continuously without personnel in the facility. Additionally, this eliminates the need to continuously remove and store classified hard drives or other processing equipment that may remain classified even when inoperative.

Example:

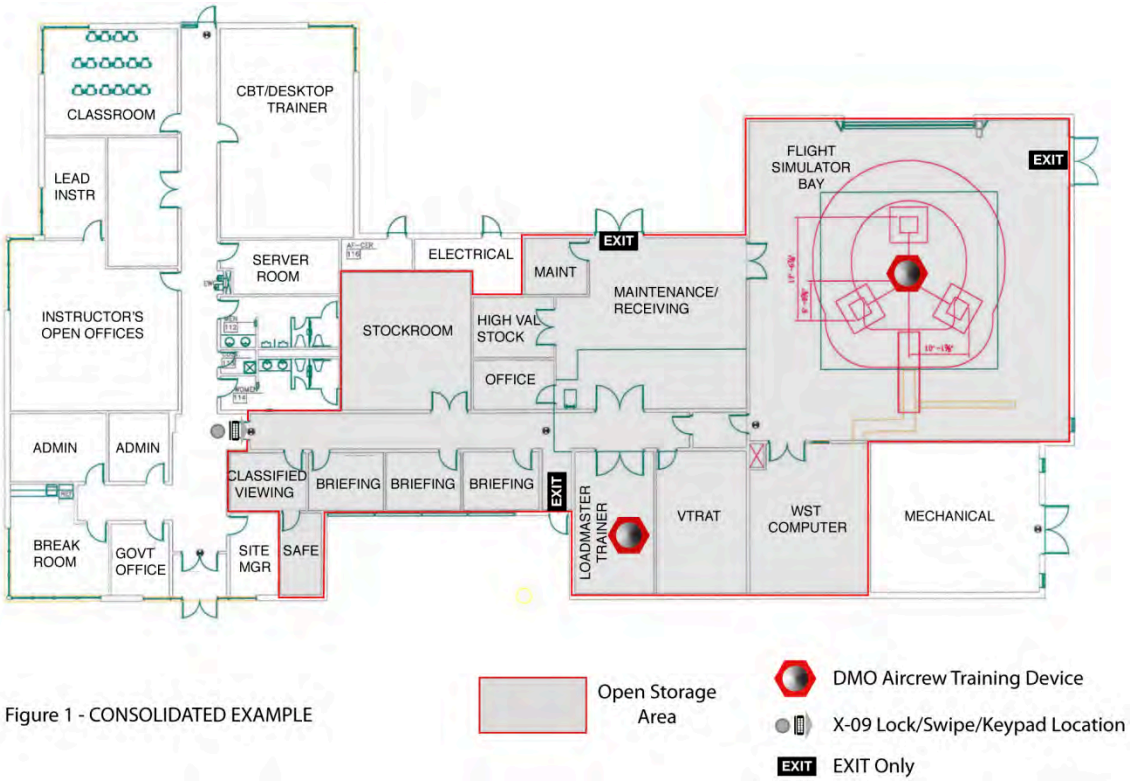

Figure 1 - CONSOLIDATED EXAMPLE

Figure 1 shows the physical security layout of the Dover AFB C-17 ATS facility. The red line (Open Storage Area perimeter) indicates how the current facility implements the consolidated option. The flight simulator bay, computer room, loadmaster trainer room, VTRAT, and all briefing rooms, plus the associated maintenance areas, are accessible only through an X-09 lock and single card swipe/key pad controlled entrance into the central hallway. Unclassified CBT rooms, restrooms, and administrative areas are outside the Open Storage Area perimeter, as are facility electrical and mechanical rooms. Three exterior exit doors plus the simulator bay "garage door" and the interior hallway door are properly constructed and alarmed. Sound attenuation testing for the classified viewing room is required since it abuts an unsecured area.

2. **Compartmentalized Option:** In this example, classified operations within an ATS facility cannot be consolidated behind a single Open Storage Area perimeter. This may be due to the fact that the physical layout of the facility is not conducive to including classified CBTs, VTRAT, and/or classified briefing rooms within the Open Storage Area. Nevertheless, the simulator bay(s) and direct support rooms that process classified information (e.g., host computer room), along with any brief/debrief rooms where host computer data is used in recreation of missions will be contained in the Open Storage Area perimeter. It is recommended that high traffic/routine maintenance rooms be included within the perimeter for practical reasons.

Example:

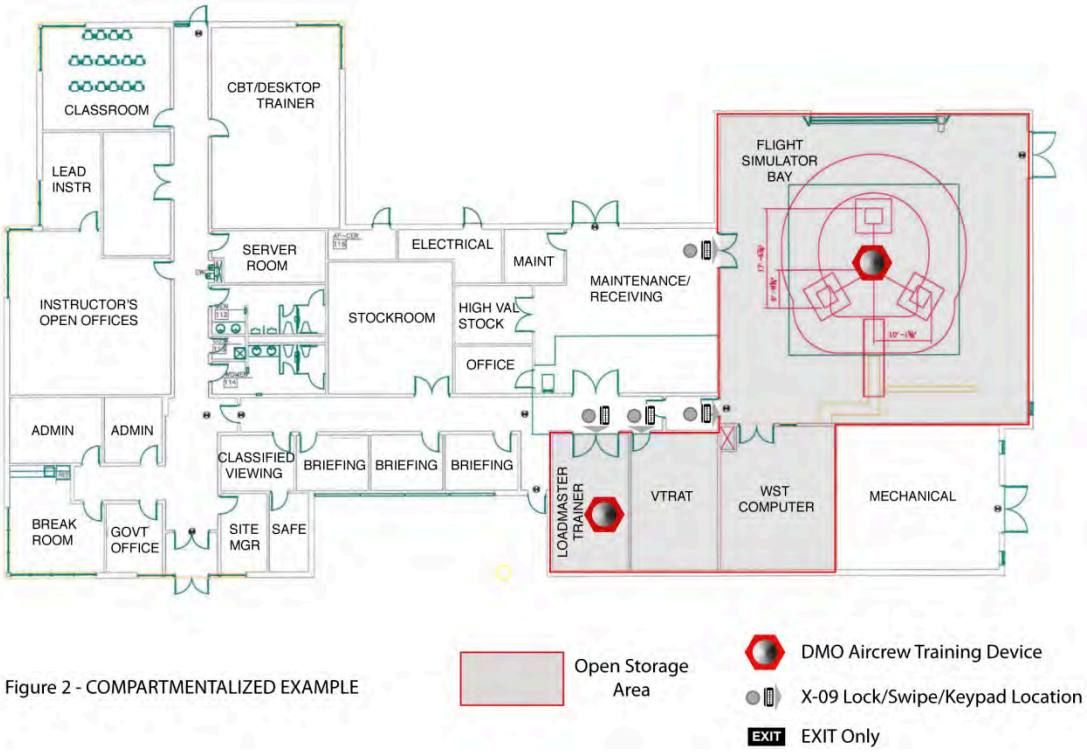

Figure 2 - COMPARTMENTALIZED EXAMPLE

Figure 2 shows the same facility in a compartmentalized configuration. In this example, *as a minimum*, the area outlined in red (simulator bay, computer room, loadmaster simulator room, and VTRAT room) would be required to be constructed as an Open Storage Area. This configuration would require additional locks and alarms to protect the loadmaster trainer room and VTRAT room, and would require locating locks at the maintenance and hallway entrances to the simulator bay. Additional sound attenuation testing/measures would be required for the VTRAT, loadmaster simulator, and classified viewing rooms (and any other rooms where discussions would possibly take place) since they would (in this configuration) abut unsecured areas.

Construction Standards for Open Storage Areas

Existing facilities/areas/rooms and new construction should comply with these standards:

Walls, Floors and Roof: The walls, floors and roof construction, will consist of permanent construction design/materials which are attached to each other. All construction must be done in such a manner so as to provide visual evidence of unauthorized penetration. Walls shall be extended to the true ceiling and attached with permanent construction materials, or with mesh or 18-gauge expanded steel screen.

Ceilings: The ceiling shall be constructed of plaster, gypsum, wallboard material, hardware or any other acceptable material.

Doors: All doors along the Open Storage Area perimeter shall be metal doors in metal frames or solid core wood doors in metal frames. Entry points (preferably a single point of entry) shall be secured by an X-09 lock and shall have a card access system (CAS) in addition to the X-09 lock. All other doors along the physical security perimeter shall be exit only and shall have no external entry hardware. The hinge pins of outswing doors shall be peened, brazed, or spot welded to prevent removal. Each door along the physical security perimeter shall have a BMS and shall be covered by motion detectors as part of the IDS. If the door has a window inset, see below.

Penetrations: Duct work penetrations through the Open Storage Area perimeter with a cross sectional area greater than 96 square inches (with both dimensions greater than 6 inches) shall be man proofed by the use of 1/2 inch diameter bars. Inspection ports will be provided preferably on the secure side of the man proofing. If the inspection port is provided on the unsecured side of the man proofing, the inspection port shall be secured by a hasp and padlock. For existing buildings, duct work penetrating through the acoustical security perimeter may be protected by white noise generators, if physical means are impractical.

Windows: Windows are not recommended along the Open Storage Area perimeter. Windows along the physical security perimeter must be a non-operable type. The glazing shall be translucent or covered by blinds, drapes, or curtains to prevent the viewing of classified material from the outside. Windows shall have glass breakage detectors and shall be covered by a motion detection sensor as part of the IDS. Windows shall be a minimum of double pane glazing in a thermally broken frame. Windows that are less than 18 feet from ground level or other easily accessible means (e.g., an adjoining roof) must have protection from forced entry.

Intrusion Detection System (IDS): The Open Storage Area shall be equipped with an IDS. The IDS must have separate zones for the motion detectors, BMS, and glass breakage sensors. The Open Storage Area will have a CAS with pin access, unique to the user. The CAS will be tied to the IDS to allow access to the facility without sending a duress alarm to security forces during open operations and to allow delayed alarm

activation during opening and closing times of the Open Storage Area, so the alarm can be turned on or off as necessary. The IDS shall report to the base security forces. When the transmission line leaves the facility and traverses an uncontrolled area, Class I or Class II line encryption will be used.

Notification System: A mechanism to provide continuous notification when an uncleared visitor is in the open storage area is required. The usual system installed is the "flashing blue lights". If three or more lights can be viewed from a single point, they shall be synchronized. If this type of system is not acceptable, then another means must be employed to notify all cleared personnel that there are un-cleared personnel present in the open storage area. ATS contracts may require modification to assign escort duties to ATS contractor personnel. Janitorial services, delivery service, civic tours, etc. will require escort.

Access Control: Access control is required to prevent unauthorized access. Access control may begin at the facility entrance, but must be in place for all Open Storage Areas. Access control systems must include a card reader with pin access. Protection of the control mechanisms and the entry control database must be provided at the same security level as that of the facility. A process for updating the control database must provided which includes a procedure for removal of the individual's access authorization on departure or revocation of security clearance. Unit security managers are responsible for providing personnel eligibility updates to the facility security manager. Access records must be retained for 90 days. Records of entries shall be retained for at least 90 days or until investigations of system access has been completed.

Hardware: The DoD Physical Security Equipment Guide (UG-2045-SHR) identifies acceptable hardware and employment of that hardware for securing high value assets, material, equipment, etc.

Sound Attenuation for Classified Discussion Areas

The acoustical security perimeter walls, doors, windows, floors and ceiling, including all openings, shall provide sufficient sound attenuation to preclude inadvertent disclosure of classified discussions. Sound attenuation requirements for amplified and non-amplified speech wil be adhered to. Typical interior walls (2 sheets of 1/2" drywall on a wood stud frame) have a sound transmission class (STC) of about 33. Adding absorptive insulation (i.e., fiberglass batts) in the wall cavity increases the STC to 36-39, depending on stud and screw spacing. Doubling up the drywall in addition to insulation can yield STC 41-45, provided the wall gaps and penetrations are sealed properly. In new construction, it is preferred to use commercially manufactured duct silencers over site produced acoustical treatments or white noise generators.

Certification

The Base Security Forces, the Base Civil Engineer and the Information Assurance Office shall inspect and certify, in writing, the facility for the desired storage of classified material (preferably unattended open storage). The acoustically secure areas shall be subjectively tested to insure that intelligible speech cannot be heard outside of the space. The subjective test shall be conducted by having one person inside talking either non-amplified or amplified as required by the space. The person outside the space shall not be able to hear intelligible speech at any point. No classified processing will take place in the facility until it has received the proper certifications.

ACRONYMS

AFCAP	Air Force Certification and Accreditation Program
AFI	Air Force Instruction
ATS	Aircrew Training System
BMS	Balanced magnet strips
C&A	Certification and Accreditation requirements
CAS	Card access system
CE	Civil engineer
CBT	Computer Based Training
DIACAP	DoD Information Assurance Certification and Accreditation Process
DMO	Distributed Mission Operations
DTC	Distributed Training Center
EITDR	Enterprise Information Technology Data Repository
EMSEC	Emissions Security
GSA	General Services Administration
IA	Information assurance
IDS	Intrusion detection system
ISPM	Installation security program managers
MAF	Mobility Air Forces
SIPRNet	Secret Internet Protocol Router Network
STC	Sound Transmission Class
VTC	Video Teleconference
VTRAT	Visual Threat Recognition and Avoidance Trainers
WST	Weapon System Trainer

REFERENCES

DoD 5200.1-R: Information Security Program, Jan 97
DoD 8510.01: DoD Information Assurance Certification and Accreditation Procedures (DIACAP), 28 Nov 07
AFI 31-401: Information Security Management Program, 1 Nov 05
AFI 33-200: Information Assurance (IA) Management, 23 Dec 08
AFI 33-201V1: Communications Security (COMSEC), 1 May 05
AFI 33-203V1: Emission Security (EMSEC), 31 Oct 05
AFI 33-203V3: Emission Security (EMSEC) Counter Measures Reviews, 2 Nov 05
AFI 33-200: Information Assurance (IA) Management
AFI 33-210: Air Force Certification and Accreditation (C&A) Program (AFCAP), 23 Dec 08
AFI 71-101V3:, Air Force Technical Surveillance Countermeasure Program, 1 Jun 00
Mil-HDBK-1013/1A: Design Guidelines for Physical Security of Facilities, 15 Dec 93
TO-00-20F-2: Inspection and Preventative Maintenance Procedures for Classified Storage Containers, 1 Dec 06
UG-2045-SHR: DoD Physical Security Equipment Guide